WHAT IS CLAIMED IS:

1. A security system for use in a distributed network, comprising:

a service provider selectively accessible via a network by a plurality of end users each having an access device for accessing the network; and

a control mechanism disposed at a location of the service provider which accesses and modifies stored information on each access device of the end users to designate portions of the information to prevent access thereof by the end users.

2. The system as recited in claim 1, wherein the stored information includes a configuration file for the access device.

3. The system as recited in claim 1, wherein service provider includes a security code for the designated portions to prevent access thereof by the end users.

4. The system as recited in claim 3, wherein the security code is associated with the designated portions at or before initializing the access devices.

5. The system as recited in claim 3, wherein the security code is associated with the designated portions after initializing the access devices.

6. The system as recited in claim 1, wherein service provider includes security levels for the information to prevent access thereof by the end users.

7. The system as recited in claim 6, wherein the security levels are associated with the designated portions at or before initializing the access devices.

8. The system as recited in claim 6, wherein the security levels are associated with the designated portions after initializing the access devices.

9. The system as recited in claim 1, wherein the control mechanism includes a software program for accessing and modifying the information of the access devices and designating portions thereof to prevent access by the end users.

10. A method for maintaining system security for a network service provider, comprising the steps of:

providing a control mechanism for remotely accessing and modifying end user network access devices;

remotely accessing and modifying the end user network devices to designate information stored on the access devices; and

preventing the end user from accessing the designated information on the end user's access device.

11. The method as recited in claim 10, wherein the step of providing the control mechanism includes providing a software program for accessing and modifying the information of the access devices and designating portions thereof to prevent access by the end users.

12. The method as recited in claim 10, wherein the step of remotely accessing and modifying the end user network devices includes remotely accessing the end user devices from a service provider's location.

13. The method as recited in claim 10, wherein the information stored on the network access devices includes a configuration file for the access device.

14. The method as recited in claim 10, wherein the step of preventing the end user from accessing the designated information includes employing a security code for the designated portions to prevent access thereof by the end users.

15. The method as recited in claim 14, wherein the security code is associated with the designated portions at or before initializing the access devices.

16. The method as recited in claim 14, wherein the security code is associated with the designated portions after initializing the access devices.

17. The method as recited in claim 10, further comprising the step of assigning security for the stored information to prevent access thereof by the end users.

18. The method as recited in claim 17, wherein the security levels are associated with the designated portions at or before initializing the access devices.

19. The method as recited in claim 17, wherein the security levels are associated with the designated portions after initializing the access devices.